Written Testimony of Amy Cohen
Executive Director
National Association of State Election Directors

United States Senate Select Committee on Intelligence
March 21, 2018

Thank you Chairman Burr, Vice Chairman Warner, and distinguished committee members for the opportunity to submit this testimony on behalf of the National Association of State Election Directors (NASED). My name is Amy Cohen, I am the Executive Director of NASED.

NASED members are the state election directors in all 50 states, the District of Columbia, American Samoa, the Commonwealth of the Northern Mariana Islands, Guam, Puerto Rico, and the U.S. Virgin Islands. Our members are the nonpartisan professionals who administer and implement election-related policies, procedures, and technologies, and NASED's mission is to promote accessible, accurate, and transparent elections in the United States and the territories, which we do by sharing information and best practices across our jurisdictions. Since elections were designated critical infrastructure in January 2017, our efforts have become more important than ever before.

In June 2017, Michael Haas, the former Administrator of Elections for Wisconsin testified before this committee on behalf of NASED and shared several of the lessons learned from 2016. As Mr. Haas discussed at that time, there are significant differences in election administration across the states. In 40 states, the secretary of state or lieutenant governor is the state's chief election official, and in the remainder, the chief election official is the Executive Director of a board or commission. Beyond differences in leadership and other obvious differences in policy, the states also differ in the way elections are conducted – in eight states, elections are conducted at the township level instead of at the county level; Wisconsin alone has 1,853 local clerks responsible for conducting elections, in addition to the state election office. I highlight these differences as a reminder of how complex the administration of elections truly is.

While I sit here today representing an incredibly diverse group, every state election official is a planner. They have spent every day since the 2016 election learning how to improve for the future, and the critical infrastructure designation has given us access to resources many did not know were available previously.

Mr. Haas' testimony last year focused on three key lessons from the 2016 presidential election. First, he noted that state election offices faced a new challenge of communicating not just with their local election officials, but also with employees of the Department of Homeland Security (DHS), who in 2016 were brand new to the nuances and complexities of election administration. Second, he noted that 2016 highlighted additional steps that states can take to secure their voter registration databases and tools they can use to improve their voter registration lists. Finally, he discussed the ongoing efforts that state and local election officials take to secure equipment used to cast and count ballots.

We are now approximately 15 months into the designation of elections as critical infrastructure, and nearly nine months removed from Mr. Haas' testimony. As a field, we have made great strides in that time.

For state election directors, communication is a significant part of the job. They must communicate basic information to their voters to ensure that every eligible voter who wants to cast a ballot can do so, and election officials must give them confidence that their vote will then be counted as they intended. Effective communication with local election officials, who serve as the boots on the ground in running elections, is also paramount. States run regular trainings and provide information and resources year-round every year to make sure that local officials have access to the information, tools, and skills they need to do their jobs effectively. Most voters will not interact with state-level election officials directly, but will with their local election official, so it is important that everyone act as a team. And, state election directors must communicate with our colleagues in the federal government. Until 2016, this was primarily with members and staff of the Election Assistance Commission (EAC), who provide an invaluable service to our field through their guides and best practices informed by both qualitative and quantitative data.

Communication with DHS, however, was new to NASED members in 2016, and is an area where we have seen significant improvement. In October 2017, DHS, the National Association of Secretaries of State (NASS), NASED, and local election officials convened the first meeting of the Government Coordinating Council (GCC) as a mechanism for sharing information about elections infrastructure threats across state, local, and federal governments. Since then, the GCC has met several times by telephone and again in-person at the NASS and NASED Winter Conferences here in Washington, D.C. last month; the Executive Committee of the GCC, which has representatives from NASS, NASED, local election official organizations, and DHS, meets every other week by telephone.

The GCC voted unanimously in February to adopt goals and objectives for the Elections Infrastructure Sector, and working groups are doing the challenging work of writing a strategic communications plan to develop guidelines and norms around communications and of writing a Sector Specific Plan to formalize the strategic goals of the Elections Infrastructure Sector for the next several years. In addition, the Elections Infrastructure Sector Coordinating Council (SCC) was launched in December 2017 with representatives from 25 private sector vendors and nonprofit organizations. The GCC and the Executive Committee of the GCC are critical to distributing information to all 50 states, the District of Columbia, and the territories, as well as disseminating critical cybersecurity information to the more than 8,000 local election officials.

The GCC also voted at the February meeting to formally recognize the Multi-State Information Sharing and Analysis Center (MS-ISAC) as the Elections Infrastructure ISAC (EI-ISAC). The purpose of an ISAC is to serve as a central resource for gathering, analyzing, and disseminating information related to critical infrastructure, and to facilitate two-way cybersecurity threat information sharing between the public and the private sectors. While all 50 states, the District of Columbia, and the U.S. territories were members of the MS-ISAC prior to 2017, election offices were not privy to the information shared by the ISAC and thus could not act on any information shared about the 2016 election. As of today, however, the EI-ISAC, which is free

for election offices to join, counts 38 state-level election offices and more than 100 local election offices as members. NASS, NASED, and the Executive Committee of the GCC strongly encourage all state and local election jurisdictions to join and are developing a strategic outreach plan to make sure every one of our state and local election officials understands the benefits of participation and joins.

DHS has also facilitated secret-level security clearances for State Chief Election Officials, as well as additional state election office staff, including state election directors. Our hope in doing so is to ensure that any future information sharing will not be hindered or delayed by the information's classification. As you are aware, processing for security clearances can take time, but we continue to make progress with DHS in this area.

Finally, DHS hosted more than 60 election directors and staff representing 43 states, the District of Columbia, and two territories for a secure briefing with the Office of the Director of National Intelligence and the Federal Bureau of Investigation in conjunction with our February conference. It would be naïve to say that we received answers to all of our questions, but the briefing was incredibly valuable and demonstrated how seriously DHS and others take their commitment to the elections community, as well as to our concerns.

There have, of course, been challenges as we have worked with DHS, but we have taken incredible leaps forward in a relatively short amount of time.

Since the November 2016 election, states have hardened the defenses of their voter registration databases and other IT systems against intrusion. This has included taking advantage of free resources such as vulnerability and risk assessments from DHS, cybersecurity services offered by state branches of the National Guard, and utilizing services offered by other branches of state government. Several private sector vendors, including Cloudflare and Google, have made tools and resources available to state and local election officials, providing additional defenses. The Defending Digital Democracy Project of the Belfer Center at Harvard and the Center for Internet Security have provided practical guidance and tools for state and local election officials to use to strengthen their cyber security posture. Election officials have long taken steps to build resiliency and redundancy into their systems, and all states are evaluating the steps they take in light of the cybersecurity threats we face today.

In addition, states continue to explore means to improve their voter registration list maintenance practices. While those of us in the field know to update our voter registration record in the event of a move or a life change, many Americans do not know to do this, or they think that updating their information with one government agency updates it at all government agencies. Inaccurate lists cause a variety of administrative headaches but can also make it easier to misuse outdated voter records.

Aging voting equipment has been at the forefront for election officials for years; the Presidential Commission on Election Administration (PCEA) report, released in 2013, highlighted the "impending crisis in voting technology" and we are now several years from that. The voting technology problem and its effect on cybersecurity is multifaceted.

First, I mentioned earlier that states run their elections differently; in some states, this extends to voting machines. In practice, this means that in some states, the state purchases voting equipment for all of its local election jurisdictions, while in other states, each county is responsible for its own election technology purchases. Local election officials are strapped for resources and are sometimes reliant on vendors or contractors for IT support. Combined, this can make it difficult for local jurisdictions to make smart technology purchases and adds an additional layer of complexity to maintaining a defensive cybersecurity posture. However, the national focus on election cybersecurity has given state and local election officials access to more information and experts. Many are taking advantage of in-state academics or national resources, including those at the EAC, to make sure that technology purchases comply with best practices.

Second, many jurisdictions purchased their current voting equipment with federal funds received via the Help America Vote Act of 2002 (HAVA), meaning that the equipment and software often predate parts of our lives we now take for granted, such as smartphones. Without additional funding, jurisdictions cannot afford to purchase new technology and are stuck trying to maintain old equipment and software on outdated, insecure operating systems. At the state and local level, elections must compete for funding with education and public safety to name just a few. We are encouraged to hear that Congress may release the outstanding HAVA funds in the Omnibus Appropriations bill.

Third, a handful of states still use voting technology that does not have a paper record or a Voter Verified Paper Audit Trail (VVPAT). These states are reliant on the accuracy of their voting machines because in the event of a recount, the records only exist in the machine. Claims abound that these machines are susceptible to malicious attack because there is no paper trail or opportunity for the voter to verify that their ballot was cast as intended. To be clear, we have seen no evidence that voting machines or election results have been manipulated or compromised in any election, but election officials must remain vigilant.

Understanding these risks is important, but we should not overlook the safeguards currently in place to protect the existing technology.

- Elections are decentralized. There are thousands of election jurisdictions, hundreds of thousands of voting locations, and many more hundreds of thousands of voting machines. The diversity of equipment used and the sheer number of precincts creates obstacles to a large-scale attack on voting equipment.

- Voting machines themselves are not connected to the internet, making them less susceptible to intrusion.

- Results released on election night are not the official results. Every state – and every local jurisdiction for elections run at the local-level – conducts an official canvass of results several days after Election Day to complete the official tally of results. In addition, an increasing number of states are doing post-election audits, the most basic of which randomly select precinct results and contest results to compare hand-counted results to the machine results. Still other states are doing Risk Limiting Audits, pioneered

by Colorado, in which statistical methods are used to select the number of ballots that must be examined for a particular contest.

In summary, the field of election administration has made great strides since the 2016 presidential election. State and local election officials cannot do this alone; if 2016 taught us anything, it is that we need a whole of government approach, with strong coordination and communication across the federal, state, and local players.

Thank you for the opportunity to share NASED's thoughts and opinions with you. I am happy to answer any questions.

####